SECTION IX. HANDLING AND CONTROL OF CONTROLLED CRYPTOGRAPHIC ITEMS DURING DEVELOPMENT AND MANUFACTURE/ASSEMBLY

63. Background and Scope.

a. Background. The concept of a Controlled Cryptographic Item (CCI) was introduced in March 1985 with the issuance of National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4001, "Controlled Cryptographic Items." It was designed to facilitate the production, acquisition, and use of Communications Security (COMSEC) equipment. CCIs are endorsed by the NSA for use in telecommunications and automated information systems to secure classified as well as sensitive information. CCIs are so designated because they either embody classified cryptographic or other classified COMSEC designs, or because they perform critical COMSEC ancillary functions (e.g., certain key fill devices).

b. Scope. This section sets forth the Government requirements for the handling and control of CCIs which embody classified cryptographic or other classified COMSEC designs during their development and manufacture/assembly. These requirements do not apply to COMSEC ancillary devices designated CCI that do not embody classified COMSEC designs (e.g., certain key fill devices).

64. Requirements.

a. Development. Normally, all phases of development of the COMSEC functions for a CCI, including the fabrication of developmental models, will be classified. However, the fabrication of developmental models need not be classified if the controls set forth in this section are applicable and are applied. Exceptions will be handled on a case-by-case basis and must be approved by NSA. Handling and control of classified information must be in accordance with the ISM and this Supplement.

b. Embodiment of Classified COMSEC Functions. The embodiment of classified COMSEC functions in a CCI will afford protection to these functions as specified below:

(1) Hardware Embodiments. Unless it can be demonstrated that it is technically not feasible to do so, hardware embodiments of classified COMSEC functions will be in custom microcircuit form; i.e., embodiments composed of discrete components and/or standard microcircuits are not permitted. In addition, the microcircuit chips must be protectively coated by an NSA-approved process which will resist recovery of classified design information by reverse engineering, unless, as verified by the NSA Program Manager (PM), one of the following applies:

(a) The protective coating is incompatible with the microcircuit chip and the reduced effectiveness inherent with the use of the coating is unacceptable.

(b) The production contract for the microcircuit was in process as of 16 January 1987 and retroactive coating would jeopardize the timely production or employment of the product to the extent that a waiver is warranted for the initial production requirement. Subsequent production requirements will include the coating unless additional waivers are obtained.

(c) Other equally protective measures have been adopted to resist reverse engineering.

(2) Firmware Embodiments. Firmware embodiments of classified COMSEC functions must be in microcircuit form (custom or standard) and must:

(a) Employ an irreversible security feature that prevents both readout and modification of the programmed information in the on-board memory from external, physically accessible pins; and

(b) The microcircuit chips must be protectively coated by an NSA-approved process which will resist attempts to defeat the security feature or to otherwise recover information in memory (e.g., by external probing). The requirement for protective coating may be waived when, as verified by the NSA PM, one of the following applies:

(1) The protective coating is incompatible with the microcircuit chip and the reduced effectiveness inherent with the use of the coating is unacceptable.

(2) The production contract for the microcircuit was in process as of 16 January 1987 and retroactive coating would jeopardize the timely production or employment of the product to the extent that a waiver is warranted for the initial production requirement. Subsequent production requirements will include the coating unless additional waivers are obtained.

(3) Other equally protective measures have been adopted to resist attempts to defeat the security feature or to otherwise recover information in memory (e.g., by external probing).

65. Manufacture and Assembly in Production. The manufacture and assembly of a CCI equipment in production may begin with either:

a. A classified design which goes through a transition during production and becomes a CCI component or assembly which the vendor further processes into a CCI equipment; or

b. A CCI component or assembly which the vendor receives from an authorized source and further processes the component or assembly into a CCI equipment.

The following paragraphs describe the handling and control requirements when the starting point is a classified design. They also cover the handling and control requirements when the starting point is a CCI component or assembly, or when the final manufactured product is a CCI component or assembly.

66. Transition from Classified to CCI. When the manufacture and assembly process begins with a classified design, the transition from classified to CCI will be as set forth below.

a. Hardware Embodiments. For hardware embodiments, the transition from classified to CCI will occur at the microcircuit photomask stage. Design automation by-products leading to and including the reticle for each layer of the microcircuit must be handled at the same classification level as the engineering drawings from which they were derived. The photomasks ultimately used as tooling in the actual production process, as well as the resulting semiconductor wafers and their subsequent forms (e.g., individual chips), leading to sealed devices, will be controlled as CCI material as set forth in this section.

b. Firmware Embodiments. For firmware embodiments, the transition from classified to CCI will occur after the classified design information has been entered into the microcircuit memory, and the security feature described in paragraph 64b(2) has been set. Thereafter, the microcircuits will be controlled as CCI material as set forth in this section. Software source data for firmware embodiments of classified design information remain classified and must be safeguarded in accordance with this Supplement.

67. Access.

a. Access to classified COMSEC information will be restricted in accordance with the provisions of this Supplement.

b. Access to CCI material will be restricted to U.S. citizens whose duties require such access. Non-U.S. citizens, including immigrant aliens, may be authorized access to CCIs and other unclassified COMSEC information and material in the manufacturing and assembly process only with the prior written approval of NSA. Such access will only be permitted when it is determined by NSA that adequate security protection exists.

68. In-Process Controls. Following the transition from classified to CCI as described in paragraph 66, CCI material must be controlled throughout the remainder of the manufacturing and assembly process as set forth in this section.

a. Microcircuit Devices. Photomasks and wafers will be marked “CONTROLLED CRYPTOGRAPHIC ITEM” or "CCI", and each must bear a serial number for accounting purposes. The marking and serial number must be legible with the naked eye. Photomasks and wafers will be accounted for by serial number: the photomasks until they are securely destroyed and the wafers until they are diced. After the wafers are diced, accounting for chips by quantity is sufficient. When the microcircuit is completely fabricated, if it is an end item for shipment, then accountability will be in accordance with paragraph 73. Otherwise, it is maintained in the vendor’s in-process accounting system as it moves to the next level of assembly. Labeling of CCI components is covered in paragraph 77.

b. Printed Wiring Assemblies. A printed wiring assembly (PWA) assumes CCI status when a CCI microcircuit is installed on it. At that point, accountability for the microcircuit ceases and accountability for the PWA begins. This disposition of the microcircuit and accountability for the PWA must be reflected in the in-process accounting records. During further assembly, PWAS will be accounted for by quantity. When the PWA is completely fabricated, if it is an end item for shipment, then accountability will be in accordance with paragraph 73. Otherwise, it is maintained in the vendor's in-process accounting system as it moves to the next level of assembly. Completely fabricated PWAs are accountable by quantity when they fit the definition of "CCI " component and by serial number when they fit the definition of "CCI assembly". (Refer to paragraph 77 for definitions of these terms.) Labeling of CCI components and assemblies is also covered in paragraph 77.

69. In-Process Procedures

a. Prior to commencing the manufacturing and assembly process for hardware embodiments, or the programming of microcircuits for firmware embodiments, the vendor must prepare detailed, written procedures to satisfy the in-process accounting requirements of this Section.

b. The procedures will provide for continuous tracking of each category of material (photomasks, wafers, microcircuit chips, finished microcircuits, printed wiring assemblies) as the material moves through the manufacturing and assembly process.

c. The accounting system must be capable of detecting a loss and identifying the work station at which the loss occurred as well as the individual(s) operating the work station at the time of the loss.

d. The procedures must provide specific instructions for the methods of control, the proper records to be maintained, and instructions for the reconciliation of in-process accounting records (refer to paragraph 76).

e. The procedures will identify the individuals or departments responsible for ensuring that the in-process accounting requirements are followed. Vendor employees which act in this capacity must be U.S. citizens.

f. The procedures must demonstrate that the vendor understands the accounting requirements.

g. Ninety days prior to start of production and implementation of the procedures, a draft must be forwarded to the NSA Project Manager for approval. Revision of the procedures require NSA approval prior to implementation. Production will not begin until NSA has approved the procedures.

h. Upon request, NSA will review the vendor's normal in-process accounting procedures for compliance with these requirements and provide guidance on adaptation of those procedures to meet NSA requirements.

70. Required Item Information. To be effective, the control system must track material in manageable units of production (e.g., lots, runs) that can each be uniquely identified in accounting records. The accounting records must indicate, as a minimum, the following information:

a. Date the material was introduced into the in-process accounting system within the facility.

b. Identification of the material to be controlled. This may be one or a combination of the following, as applicable:

(1) Federal stock number.

(2) NSA or Vendor part number.

(3) NSA short title (trigraph).

c. Quantity, when accounting by quantity, or serial number if individual item accounting is required.

71. Breakage and Scrap. It is recommended that any area in which breakage of a CCI wafer has occurred be immediately safeguarded and every effort made to reconstruct the broken wafer onto an adhesive base. If, however, any portion, or the entire wafer, has fragmented to such a degree that reconstruction is impossible, it is recommended that all particles be removed from the breakage area by vacuuming. All materials under in-process accounting controls which leave the manufacturing and assembly process due to failure or breakage and normally occurring waste (e.g., broken wafer, partial die, etc.) must be controlled until securely destroyed as set forth in paragraph 74. In-process accounting records must reflect the failure or breakage.

72. Loss of In-Process Controlled Material. A reasonable search must be made for lost items which are under in-process accounting controls. All such losses must be documented in the vendor's records and must be reported to NSA (S213) within 24 hours of discovery of the loss. During normal duty hours, telephone (301) 688-6010. After normal duty hours, telephone the Senior Information Security Coordinator at (301) 688-7003. A written follow-up report shall be submitted within 30 days to NSA (S213). The written report shall include identification of the item involved, a description of the incident (when, where, and what happened; who discovered the loss; etc.), conclusinos as to the cause, and actions taken to prevent future occurence.

73. Transition from In-Process Controls to Control Within the Formal COMSEC Accounting System. Upon completion of the manufacturing and assembly process, CCI equipments, assemblies, and components which are destined for sale to authorized buyers will transition from in-process accounting controls into the formal COMSEC accounting system, and will be picked up in the vendor's COMSEC account. The transition will be reflected in the vendor's in-process accounting records. However, CCI components and assemblies produced by a subcontractor and provided to the vendor will not be entered into the formal COMSEC accounting system by the vendor. Instead, such material will be placed in the in-process accounting system by the vendor and controlled in accordance with this section. CCI equipments and assemblies will be accounted for by serial number; CCI components will be accounted for by quantity.

74. Destruction of CCI Materials. All material designated CCI which leaves the manufacturing and assembly process due to unserviceability (e.g., faulty photomask), breakage/reject (e.g., broken/reject wafer, failed microcircuit), or normally occurring waste (e.g., partial die) must be securely destroyed. Secure destruction is best accomplished by high-temperature incineration (MOS

microcircuit materials require temperature on the order of 3,000 degrees F). NSA has the capability for high-volume destruction of these materials, and it is preferred that the material be forwarded to NSA for destruction. Alternatively, the vendor may elect to destroy the material locally. To do so requires the written permission of the NSA PM. Vendor requests to destroy the material locally must include a detailed description of the proposed process to be employed.

a. Destruction by the Vendor. Where material under in-process accounting controls is to be destroyed by the vendor, the material will be turned over to a U.S. citizen employee who has been designated to be responsible for the destruction operation. This person must maintain a record of the materials received for destruction. The actual destruction of all such material must be witnessed by one other designated individual who must also be a U.S. citizen. Both the person responsible for destruction and the witness will sign a local destruction record attesting to the destruction of the recorded material. Destruction records must be retained by the vendor for a minimum of two years.

b. Destruction by NSA. Where material under in-process accounting controls is to be forwarded to NSA for destruction, all like items will be packaged together (e.g., photomasks in one package, wafers in another, PWAS in another, etc.). A transmittal (SF-153) with an in-process transaction number (NOTE: Do not use a COMSEC account transaction number) will be included in each container. The transmittal will include a statement that the listed material is for destruction. Items must be identified sufficiently to allow crosschecking against the transmittal. The transmittal will be signed by two U.S.-citizen employees, designated to be responsible for this function, attesting to the accuracy of the inventory and the proper packaging of all material forwarded to NSA for destruction. The container must be securely sealed and labeled with the following address:

Director
National Security Agency
Operations Building No.3
ATTN : Y133
Fort George G. Meade, MD 20755-6000

75. Subcontracting. When awarding a subcontract which will involve the manufacture or assembly, or other handling, of CCI materials which are subject to in-process controls, the prime contractor must require that the subcontractor develop in-process accounting procedures and will submit them on the subcontractor's behalf to NSA for approval. The prime contractor will ensure that the requirements for in-process accounting, as well as all other applicable requirements as set forth in this section, are specified in the contract with the subcontractor. In-process controlled material must not be released to, or produced by, the subcontractor until NSA has approved the procedures.

76. Reconciliation of In-Process Accounting Records. Both vendor and subcontractor are required to reconcile their own in-process accounting records and to perform a records reconciliation between each other to ensure accountability for all in-process controlled material. Reconciliation must

be effected at least semiannually and at the conclusion of all work on a particular item. Any shortage discovered as a result of the records reconciliation process must be documented in the vendor's records and is reportable as loss in accordance with paragraph 72. The individuals performing the reconciliation must be U.S. citizens and records attesting to the accuracy of the reconciliation will be signed by them. These records must be retained by the vendor for a minimum of two years.

77. Labeling of Components, Assemblies, and Equipments. CCI components, assemblies, and equipments will be labeled "CONTROLLED CRYPTOGRAPHIC ITEM" or "CCI" in accordance with standard drawings available from NSA and the following:

a. CCI components 1/ will be labeled "CCI" at the same time as other part-specific nomenclature is applied.

b. CCI assemblies 2/ will be labeled "CONTROLLED CRYPTOGRAPHIC ITEM" (space permitting) or "CCI" otherwise. CCI assemblies will also bear a government serial number (GSN) for accounting purposes, in accordance with the criteria to be furnished by NSA. Labeling may be applied at any stage of the assembly process, but must be applied by the end of the assembly process. CCI controls applicable to the assembly need not take effect until a CCI component is installed.

c. CCI equipments 3/ will be labeled "CONTROLLED CRYPTOGRAPHIC ITEM" in a conspicuous external location. CCI equipments will also bear a GSN for accounting purposes, in accordance with criteria to be furnished by NSA. Labeling may be applied at any stage of the assembly process, but must be applied by the end of the assembly process. CCI controls applicable to the equipment need not take effect until a CCI component or assembly is installed.

1/ A CCI component is a device which embodies a cryptographic logic, or other COMSEC design, approved by NSA for designation as a CCI, where the device does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete the COMSEC function as well as to operate.

2/ A CCI assembly is a device which embodies a cryptographic logic, or other COMSEC design, approved by NSA for designation as a CCI, where the device performs the entire COMSEC function but is dependent upon the host equipment to operate.

3/ A CCI equipment is a telecommunications or information handling equipment which embodies a CCI-designated component or assembly and which performs the entire COMSEC function without dependence on a host equipment to operate.

78. Auditing' of In-Process Accounting Records. Audits of vendor and subcontractor in-process accounting records will be conducted by NSA annually or as deemed necessary. The vendor muse make provisions in the contract for NSA to audit the in-process accounting records of subcontractors. Written records indicating the results of the in-process accounting reconciliations at the vendor or between the vendor and its subcontractor, as well as documentation of lost, broken, scrap, or destroyed CCI material, must be made available to NSA during audits.